REMARKS

Applicant acknowledges, with thanks, the Office Action mailed October 18, 2004. This Amendment and Response is responsive to the Final Office Action mailed October 18, 2004. The three month shortened statutory period expired January 18, 2005, accordingly a petition and fee for a one month extension along with a Request for Continued Examination (RCE) is being submitted with this amendment and response.

By this amendment, claim 6 and 9 have been amended, and claims 83-86 have been added. No new matter has been added, the key exchange procedure is disclosed in the original specification in Figures 21 and 22. The element of checking a queue limit counter, and aborting the process and writing an error log entry is not new matter as it is disclosed in Figure 23 of the original specification. Claims 8 and 11-12 have been cancelled.

THE REJECTIONS UNDER 35 U.S.C § 102

Claims 6-59 had been rejected under Section 102(e) as being anticipated by Vasic et al. (U.S. Publication No. 2003/0021417). Applicant acknowledges, with thanks, the receipt of the Madoukh publication (U.S. Publication No. 2001/0019614), the parent application of the Vasic reference.

A. Applicant conceived invention before effective data of Madoukh and exercised diligence in filing application.

As demonstrated in the attached Declaration of Marcia R. Kirby, one of the inventors of this application, pursuant to 37 C.F.R. 1.131 (hereinafter the "Kirby Declaration"), and accompanying exhibits, applicant believes that the applicant's conception of the invention occurred prior to the effective date of the Madoukh reference. As the exhibits illustrate, applicant conceived the subject invention on or before September 7, 2000, approximately one month prior to the effective date of October 20, 2000 of the Madoukh reference. In addition, the applicant, as illustrated in the attached Kirby Declaration and accompanying exhibits, believes to

have demonstrated due diligence from the date of conception to the filing date of April 17, 2001 of the subject application.

Therefore, applicant believes that the rejection of the subject application based upon the Madoukh reference has been traversed. Accordingly, applicant respectfully submits that claims 6-59, as listed above, are not anticipated and that the present claims are in condition for allowance.

B. Claim 6 as now amended and new claims 83-86 are not anticipated by Madoukh or Vasic.

In addition to the reasons set for above, for reasons that will not be set forth claim 6 as now amended and claims 83-86 are not anticipated by Madoukh or Vasic.

Claim 6, as now amended, recites generating a first key pair by the responder, comprising a responder public key and a responder private key. Claim 6 further recites that the session confirm is sent from the responder to the initiator and contains the responder public key. Furthermore, the initiator generates a second key pair, the second key pair comprising an initiator public key and an initiator private key. When the key request is sent from the initiator to the responder, it contains the initiator public key and is encoded using the responder public key.

By contrast, only one session key pair (public and private) are used in the transactions described in Madoukh. Referring to Fig. 10, the Encryption Key manager (EKM) generates a System Encryption Key (SEK) and SEKID. The SEKID is sent with a system key and the General Security Manager (GSM) encrypts the data at step 1178, and at step 182 the encrypted data is stored. Nowhere in the process described in Figure 10 is a key exchange performed where two sets of keys are generated for the session, and the initiator and the responder exchange public keys before transferring the data as now recited in claim 6. Figure 11 describes how a user can access the data, notably, again as in Figure 10 exchange of public keys is performed, the user obtains the system private key at step 194. Likewise, in Figure 12 now public keys are

exchanged. In Figures 13 and 14, a lifetime key manager (LFM) updates keys with the GSM. However, the update does not involve any communication with the client (initiator).

Furthermore, claim 84 recites the data package is sent encoded with responder public key and the package confirm is encoded with the initiator public key. As stated hereinabove, Madoukh does not disclose using two separate keys, nor does it disclose each party (initiator and responder) encoding messages it sends with its own public key as recited in claim 84.

Therefore, for the reasons just set forth, claim 6 as now amended and claim 84 are not anticipated by Madoukh.

New claim 85 recites that the responder when the session request is received determines whether a queue limit counter has been exceeded. By contrast, the only counter Madoukh uses is described in paragraph 0061, which counts how many times a key has been used, which would be inapplicable with the present invention because a new key pair is generated for each transaction. Therefore, for the reasons just set forth, claim 85 is not anticipated by Madoukh.

In addition to the reasons set forth for claim 85, claim 86 recites aborting the method and writing an error log entry responsive to exceeding the queue limit counter. Nothing in Madoukh describes this. Therefore, claim 86 is not anticipated by Madoukh.

C. Rejection is based on material in child CIP Application (Vasic) not found in parent application (Madoukh)

In addition to the reasons already set forth, Applicant maintains that Vasic is not prior art for this application and the rejection based on Vasic is based on new matter added to Vasic and not found in Madoukh. Applicant has again carefully reviewed the disclosures of both the Madoukh publication and the Vasic publication and respectfully disagrees with the Examiner's contentions that the Madoukh publication includes sufficient disclosure to maintain the rejections of the instant claims based upon the added disclosure of the child application, Vasic. Therefore, Applicant respectfully traverses this rejection.

Applicant maintains the arguments set forth in the response to the office action received in April 2004. Vasic, a continuation-in-part of the Madoukh application, is not available as a prior art reference as the filing date of the instant application of April 17, 2001 predates the Vasic application filing date of May 15, 2002 by over a year. The Applicant's review of the Madoukh application indicates that Madoukh is directed to storing data and the encryption and decryption of data already stored in a database, *i.e.,* data at rest. The subject matter of the present invention is directed to the encryption and decryption of data in motion, e.g., data being transmitted from one computer to another as is the new matter added in Vasic.

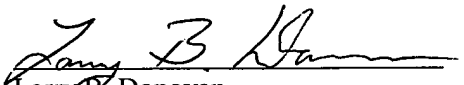
The Examiner based his rejections on paragraphs 0029-0033 and 0079 of Vasic. Of these paragraphs recited by the Examiner, only the subject matter of paragraphs 0031 and 0079 appear in Madoukh. With respect to the Examiner's claim rejections based upon the disclosure of paragraphs 0029, 0030, and 0033, of Vasic, it is respectfully submitted that the matter contained in these paragraphs fails to find support in the original disclosure of the Madoukh application. For example, Applicant has reviewed the parent application of Madoukh extensively, even searching the document online for the word "remote", which Applicant determined, is not used, even a single time, within the Madoukh parent application. Other content contained in the cited paragraphs of the Vasic reference is also lacking from the disclosure of the Madoukh application. For example, as stated in Paragraph 0029, Vasic includes a "cryptographic engine" and a "key exchange module", neither of which are present in the parent application. As previously stated, "remote" is not used in Madoukh, however paragraph 0030 of Vasic indicates the presence of a "remote data entity". Paragraph 0033 of Vasic includes a "key exchange module", "key request", an "exchange public key", and other components which are not found in the parent application. Thus, applicant hereby reiterates that a portion of the subject matter of Vasic used to reject Applicant's claims 6-59, specifically the subject matter of paragraphs 0029, 0030, and 0033, is not found within the Madoukh parent application and rather, constitutes the new matter in the continuation in part application.

It is respectfully noted that the Vasic et al. reference has a filing date of May 12, 2002, whereas the present application has a filing date of April 17, 2001. Therefore, it should be plain that Vasic et al. is not 102 prior art as applied to the present claims. It is further noted that Vasic et al. is a continuation-in-part of Madoukh filed October 20, 2000. It should be appreciated that the Vasic reference, as set forth in detail above, contains new matter and includes only a portion of disclosure that can draw from this earlier date. It is now clear from the Examiner's remarks and a careful review and analysis of the Madoukh and Vasic applications that a portion of the matter forming the outstanding rejection is based on portions of the Vasic reference having a later filing date than the present application. Thus, Applicant respectfully submits that it has not been established that this reference and the cited portions relied upon do in fact anticipate the present claims. It is therefore respectfully submitted that the burden of proof has not been met in this outstanding rejection. Since an earlier date cannot be established on the outstanding rejection, it is respectfully submitted that the claims distinguish over the Madoukh. reference. Withdrawal of this rejection and an indication of allowability is therefore respectfully requested.

CONCLUSION

In view of the foregoing it is respectfully submitted that the present claims distinguish over the prior art. If the Examiner believes there are any further matters, which need to be discussed in order to expedite the prosecution of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,
TUCKER ELLIS & WEST LLP



Larry B. Donovan
(Registration No. 47,230)
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
216-696-3864 (phone)
216-592-5009 (fax)